SYSLOG-2

syslog() is subject to format string vulnerabilities.

Sean Barnum, Cigital, Inc. [vita[1]]

2007-04-23

Part "Original Cigital Coding Rule in XML"

Mime-type: text/xml, size: 3619 bytes

Attack Category	• Malicious Input
Vulnerability Category	• Format string • Buffer Overflow • Unconditional
Software Context	• Logging
Location	
Description	syslog() is subject to format string vulnerabilities.
APIs	**Function Name** / **Comments** syslog vsyslog
Method of Attack	Use of syslog() can introduce vulnerability to a format-string attack. syslog() is used to log system message. syslog() accepts a printf-style format string as a parameter for it's messages. Because of this, an attacker could potentially send a message that could cause syslog to fail.
Exception Criteria	
Solutions	**Solution Applicability** / **Solution Description** / **Solution Efficacy** When syslog is used. / Verify that input is of a limited size. If the message is coming from an outside source, check for %s type parameters and ensure that bounds will not be overwritten. Don't use text from an outside / Effective.

1. http://buildsecurityin.us-cert.gov/bsi-rules/35-BSI.html (Barnum, Sean)

	source as a format string.
Signature Details	void syslog(int priority, char *format, ...)

Examples of Incorrect Code	`[...]`
	`openlog("my_program", 0, LOG_USER);`
	`void syslog( LOG_WARNING, textAHackerCouldInfluence);`
	`closelog();`
	`[...]`

Examples of Corrected Code	`[...]`
	`openlog("my_program", 0, LOG_USER);`
	`/* Truncate text to ensure not too big. If syslog() formatting supports it, could alternatively use formatting options that limit output size. */`
	`char textBuffer[MAX_SAFE_TEXT_SIZE]; /* Safe size depends on syslog() implementation */`
	`strncpy(textBuffer,textAHackerCouldInfluence`
	`textBuffer[sizeof(textBuffer)-1] = '\0';`
	`void syslog( LOG_WARNING, "%s", textBuffer);`
	`closelog();`
	`[...]`

Source Reference	• Viega, John & McGraw, Gary. *Building Secure Software: How to Avoid Security Problems the Right Way*. Boston, MA: Addison-Wesley Professional, 2001, ISBN: 020172152X, p. 148.
Recommended Resource	• Syslog man page[2]
Discriminant Set	**Operating System**: • Windows **Languages**: • C • C++

Cigital, Inc. Copyright

The Build Security In (BSI) portal is sponsored by the U.S. Department of Homeland Security (DHS), National Cyber Security Division. The Software Engineering Institute (SEI) develops and operates BSI. DHS funding supports the publishing of all site content.

1. mailto:copyright@cigital.com